第五章 代数结构

5.1 代数系统的引入

集合上的运算

例如：

R上的1/a (a!=0) 一元的

R上的a+b 二元的

R上的if a=0 then b else c 三元的

共同的特征：运算结果也属于R——封闭性。

代数系统

定义5-1.1 对于集合A，一个从A^n到B的映射，称为集合A上的一个n元运算。如果B是A的子集，则称该n元运算是封闭的。

定义5-1.2 一个非空集合A连同若干个定义在该集合上的运算$f_1,f_2,\cdots,f_n$所组成的系统就称为一个代数系统，记作〈$A,f_1,f_2,\cdots,f_n$〉。

代数系统

注：代数系统是由一个集合和定义在集合上的若干运算构成。

①集合一般是非空的，

例：整数集，实数集，符号串集合等。

②定义在集合上的n元运算是一个从A^n到B的映射。

例：

<N,+>,

<ρ(s),∪,∩,~>都是一个代数系统。

5.2 运算及其性质

对于二元运算来说

定义5-2.1：*是定义在A上的二元运算，若∀x，y∈A，有x*y∈A， 称*在A上是封闭的。

例： $A=\{2^n \mid n\in N\}$，问<A，x>运算封闭否，<A，+>，<A，/>呢？

解：

- $\forall 2^r，2^s\in A，2^r x 2^s=2^{r+s}\in A$（$r+s\in N$），∴<A，x>运算封闭。
- 2，4∈A，2+4∉A，∴<A，+>运算不封闭。
- 2，4∈A，2/4∉A，∴<A，/>运算不封闭。

交换律

定义5-2.2 *是定义在A上的二元运算，若∀x，y∈A，有 x*y=y*x，称*满足交换律。

例：设<有理数集，*>，*定义如下：

a*b=a+b-ab， 问*满足交换律否？

证：∵∀a，b∈A，

a*b=a+b-ab=b+a-ba=b*a

∴*满足交换律。

结合律

定义5-2.3 ＊是定义在A上的二元运算，若∀x，y，z∈A，有x＊(y＊z)=(x＊y)＊z，称＊满足**结合律**。

例：<A，＊>，若∀a，b∈A，有a＊b=b。

证明：＊满足结合律

证：∀a，b，c∈A，

a＊（b＊c）=a＊c=c

（a＊b）＊c=b＊c=c

∴a＊（b＊c）=（a＊b）＊c

＊满足结合律。 #

分配律

定义5-2.4 设＊和△是定义在A上的两个二元运算，若∀x，y，z∈A都有：

x＊(y△z)=（x＊y）△（x＊z）

(y△z)＊x=（y＊x）△（z＊x），

称运算＊对于运算△是**可分配**的。

例：设A={α，β}，二元运算＊和△的**运算表**如右：问分配律成立否？

＊	α	β
α	α	β
β	β	α

△	α	β
α	α	α
β	α	β

＊	α	β
α	α	β
β	β	α

△	α	β
α	α	α
β	α	β

解：验证_△（_＊_）组成的8个式子，看是否满足。

或者这样：

① 若能证x△(y＊z)=(x△y)＊(x△z)，则△对＊可分配

证：当x=α：x△(y*z)=α；(x△y)＊(x△z)=α

当x=β：x△(y*z)=y*z；(x△y)*(x△z)=y*z

②运算＊对运算△不可分配（举一个反例即可）

证：∵β＊(α△β)=β＊α=β

(β＊α)△(β＊β)=β△α=α

吸收律

定义5-2.5 设＊和△是定义在A上的两个可交换的二元运算，若∀x，y∈A有：

x＊(x △ y)=x， x △(x＊y) =x，

称运算＊和运算 △满足**吸收律**。

例:N为自然数集,∀x,y∈N，x*y=max{x，y}，x△y=min{x，y}

试证：＊和△满足吸收律。

证明：∀x，y∈N，

x＊（x△y）=max{x，min{x，y}}=x， ∴＊满足吸收律。

x△（x＊y）=min{x，max{x，y}}=x， ∴△满足吸收律。

∴＊和△满足吸收律

等幂律

定义5-2.6＊是定义在A上的二元运算，若∀x∈A，都有 x*x=x， 则称＊满足**等幂律**。

例：已知集合s，<ρ（s）,∪,∩>。

∀A，B∈ρ（s）， A∪A=A， A∩A=A

A∩（A∪B）=A，A∪（A∩B）=A

则∪和∩满足吸收律，等幂律。

幺元和零元

定义5-2.7，5-2.8 设＊是定义在A上二元运算，如果存在元素e_r，e_l，θ_r，θ_l，e，θ∈A，有

①.若∀x∈A，有e_l＊x=x，称e_l为运算＊的**左幺元**。

若∀x∈A，有x＊e_r=x，称e_r为运算＊的**右幺元**。

②.若∀x∈A，有θ_l＊x=θ_l，称θ_l为运算＊的**左零元**。

若∀x∈A，有x＊θ_r=θ_r，称θ_r为运算＊的**右零元**。

③. 若∀x∈A，有e＊x=x＊e=x，称e为运算＊的**幺元**。也叫**单位元**

若∀x∈A，有θ＊x=x＊θ=θ，称θ为运算＊的**零元**。

（以知识经验中的乘法运算为*的模型来学习，但*不一定是乘法!）

幺元和零元

例:

a) 〈I，x〉，I为整数集则幺元为1，零元为0

b) 〈ρ（s），∪，∩〉

对运算∪，∅是幺元，s是零元，

对运算∩，s是幺元，∅是零元。

c) 〈N，+〉有幺元0，无零元。

（以知识经验中的乘法运算为*的模型来学习，但*不一定是乘法!）

幺元和零元

例：代数系统A=〈{a，b，c}，*〉，* 的运算表如下：

*	a	b	c
a	a	b	b
b	a	b	c
c	a	b	a

则b是左幺元，无右幺元，

a是右零元，b是右零元，无左零元；

运算 * 既无幺元，也无零元 。

幺元和零元

定理5-2.1: 设*是定义在 集合A上的二元运算，且在A中同时存在关于*运算的左幺元e_l和右幺元e_r，则$e_l=e_r=e$，且幺元唯一。

证明： $e_r = e_l * e_r = e_l$

设有二个幺元e，e'；则e=e * e' =e'。

#

幺元和零元

定理5-2.2: 设*是定义在 集合A上的二元运算，且在A中同时存在关于*运算的左零元θ_l，右零元θ_r，则有：

$\theta_l = \theta_r = \theta$，且零元唯一。

(证明与定理5-2.1类似)

定理5-2.2: 设〈A，*〉是一个代数系统，且集合A中元素的个数大于1。如果该代数系统中存在幺元e和零元θ，则$\theta \neq e$。

证明：（反证法）设$\theta=e$，那么对于任意的$\forall x \in A$，必有

$x=e*x=\theta*x=\theta$，

于是A中的所有元素都是相同的，这与A中含有多个元素相矛盾。

逆元

定义5-2.9　设*是定义在A上的二元运算，e是运算*的幺元：

若对于元素a存在着元素b，使得b * a=e，那么称b为a的左逆元，如果a * b=e，则称b为a的右逆元。

如果一个元素b既是a的左逆元，又是a的右逆元，则称b是a的逆元。

显然，如果b是a的逆元，则a也是b的逆元，简称a与b互逆，a的逆元记作a^{-1}。

一般地，左、右逆元未必相等，左、右逆元未必存在，甚至不唯一。

逆元

例1: 代数系统〈R，×〉中，幺元为1，零元为0，除0外所有元素均有逆元。

例2： A=<{a，b，c}，* >，* 运算表由下表定义：

则指出每个元素的逆元?

*	a	b	c
a	a	a	b
b	a	b	c
c	a	c	c

解： 首先找出*的幺元: b，由此:

a的右逆元为c，无左逆元，

b的逆元为b，

c无右逆元，左逆元为a。

逆元

例1: 代数系统〈R, ×〉中，幺元为1，零元为0，除0外所有元素均有逆元。

例2：A=<{a, b, c}, *>, *运算表由下表定义：

则指出每个元素的逆元？

*	a	b	c
a	a	a	b
b	a	b	c
c	a	c	c

解：首先找出*的幺元: b, 由此:

a的右逆元为c，无左逆元，

b的逆元为b，

c无右逆元，左逆元为a。

19

逆元

例1: 代数系统〈R, ×〉中，幺元为1，零元为0，除0外所有元素均有逆元。

例2：A=<{a, b, c}, *>, *运算表由下表定义：

则指出每个元素的逆元？

*	a	b	c
a	a	a	b
b	a	b	c
c	a	c	c

解：首先找出*的幺元: b, 由此:

a的右逆元为c，无左逆元，

b的逆元为b，

c无右逆元，左逆元为a。

20

逆元

例1: 代数系统〈R, ×〉中，幺元为1，零元为0，除0外所有元素均有逆元。

例2：A=<{a, b, c}, *>, *运算表由下表定义：

则指出每个元素的逆元？

*	a	b	c
a	a	a	b
b	a	b	c
c	a	c	c

解：首先找出*的幺元: b, 由此:

a的右逆元为c，无左逆元，

b的逆元为b，

c无右逆元，左逆元为a。

21

逆元

例1: 代数系统〈R, ×〉中，幺元为1，零元为0，除0外所有元素均有逆元。

例2：A=<{a, b, c}, *>, *运算表由下表定义：

则指出每个元素的逆元？

*	a	b	c
a	a	a	b
b	a	b	c
c	a	c	c

解：首先找出*的幺元: b, 由此:

a的右逆元为c，无左逆元，

b的逆元为b，

c无右逆元，左逆元为a。

22

逆元

例1: 代数系统〈R, ×〉中，幺元为1，零元为0，除0外所有元素均有逆元。

例2：A=<{a, b, c}, *>, *运算表由下表定义：

则指出每个元素的逆元？

*	a	b	c
a	a	a	b
b	a	b	c
c	a	c	c

解：首先找出*的幺元: b, 由此:

a的右逆元为c，无左逆元，

b的逆元为b，

c无右逆元，左逆元为a。

23

逆元

例1: 代数系统〈R, ×〉中，幺元为1，零元为0，除0外所有元素均有逆元。

例2：A=<{a, b, c}, *>, *运算表由下表定义：

则指出每个元素的逆元？

*	a	b	c
a	a	a	b
b	a	b	c
c	a	c	c

解：首先找出*的幺元: b, 由此:

a的右逆元为c，无左逆元，

b的逆元为b，

c无右逆元，左逆元为a。

24

逆元

一般地，左、右逆元未必相等，左、右逆元未必存在，甚至不唯一。

定理5-2.4： 设代数系统<A,∗>， ∗是定义在A上的二元运算，A中存在幺元e，且每个元素都有左逆元。如果∗是可结合的，那么任何元素的左逆元必定也是该元素的右逆元，且逆元唯一。

证：设a，b，c∈A，b是a的左逆元，c是b的左逆元(c是构造性的)，

因为 $(b*a)*b=e*b=b$，

则 $e=c*b = c*((b*a)*b)=(c*(b*a))*b=((c*b)*a)*b$
$=(e*a)*b=a*b$，即 b也是a的右逆元。

设a有两个逆元b和c，则 $b=b*e=b*(a*c)=(b*a)*c=e*c=c$

则a的逆元唯一。

两部分证明所使用的符号是相互独立的!

从运算表中看二元运算的性质

1）运算 * 具有封闭性，当且仅当运算表中的每个元素都属于A。
2）运算 * 具有可交换性，当且仅当运算表关于主对角线是对称的。
3）运算 * 具有等幂性，当且仅当运算表的主对角线上的每一个元素与它所在的行（列）的表头元素相同。
4）A关于运算 * 有零元，当且仅当该元素所对应的行和列中的元素都与该元素相同。
5）A关于运算 * 有幺元，当且仅当该元素所对应的行和列依次与运算表的行和列相一致。
6）设A中有幺元，a和b互逆，当且仅当位于a所在行，b所在列的元素以及b所在行，a所在列的元素都是幺元。

5. 3 半群

半群是一种特殊的代数系统，在计算机形式语言，自动机理论，编码理论等得到广泛应用。

(代数系统(广群)：集合+运算+封闭)

广群和半群

定义5-3.1： 具有运算封闭性的代数系统〈S， *〉称为广群。

定义5-3.2： 满足封闭性、结合律的代数系统< S， * >，称为半群，即∀x，y，z∈S满足

$(x*y)*z=x*(y*z)$

广群：集合+运算+封闭性
半群：集合+运算+封闭性+结合律

例1、a) 〈N，+〉 〈N，x〉 是半群，

〈I_+，-〉 和 〈R，/〉？ 不是半群

b) 设s={a，b}，*定义如右表。

问：是半群吗？

*	a	b
a	a	b
b	a	b

∵∀x,y,z∈s

① x*y∈s ∴运算封闭

② 观察到y*z=z，从而：

x*（y*z）=x*z=z；（x*y）*z=z

∴结合律成立， ∴〈s，*〉是半群。

子半群

定理5-3.1 设〈S，*〉是半群，B⊆S且*在B上是封闭的，那么〈B，*〉也是一个半群。

通常称〈B，*〉是半群〈S，*〉的子半群。

证明：

因为*在S上是可结合的，而B⊆S且*在B上是封闭的，所以*在B上也是可结合的，故〈B，*〉也是一个半群。 #

该定理提供了一种构造半群的方法。

等幂元

定理5-3.2 有限半群<S,*>,则必∃a∈s，有a*a=a 。

（这样的a叫等幂元）　定义5-2.6 *是定义在A上的二元运算，若∀x∈A，都有 x*x=x， 则称*满足等幂律。

证明： ∀b∈s ，因为运算封闭，$b^2=b*b\in s$ b^3，b^4，…∈s

∵ s有限 ∴∃ *i* ，j(j> *i*) 有$b^i=b^j$。

∴ $b^i=b^j=b^{j-i}*b^i$。

∴令p=j－i 当q≥i ,$b^q=b^p*b^q$ （1）

又∵p≥1 ∴∃k 有k p ≥i ，

由（1） $b^{kp}=b^p*b^{kp}=b^p*(b^p*b^{kp})=\ldots=b^{kp}*b^{kp}$,

∴令$a=b^{kp}\in s$ 则a*a=a ∴ b^{kp}是等幂元。 #

独异点

定义5-3.3：含有幺元的半群称为独异点

（也称含幺半群）。

广群: 集合+运算+封闭性

半群: 集合+运算+封闭性+结合律

独异点: 集合+运算+封闭性+结合律+幺元

例

<R,+>; <N, x > 都是独异点，幺元分别为0和1.

<N-{0},+> 是半群，不是独异点，没有幺元

定理5-3.3 独异点<S,*>，则*运算表中任何两行或两列均不相同。(注:幺元唯一)

证明：设独异点的幺元为e，∀a，b∈s，a≠b

∵a*e≠b*e

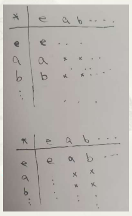
∴ < *s* ， * > 运算表中 *a* ， *b* 两行不同。

由 *a* ， *b* 任意性，运算表中任两行不同。

∵ e*a≠e*b

∴ < *s* ， * > 运算表中 *a* ， *b* 二列不同。

由 *a* ， *b* 任意性，运算表中任两列不同。



定理5-3.4 独异点〈S，*〉，a，b∈S，若a，b均有逆元，则 1) $(a^{-1})^{-1}=a$; 2) $(a*b)^{-1}=b^{-1}*a^{-1}$

证明：1) ∵$a*a^{-1}=e$ ∴a是a^{-1}的左逆元(逆元的相互性)

$a^{-1}*a=e$ ∴a是a^{-1}的右逆元

∴ $(a^{-1})^{-1}=a$

2) ∵ $(a*b)*(b^{-1}*a^{-1})=a*(b*b^{-1})*a^{-1}=a*e*a^{-1}=e$

∴$b^{-1}*a^{-1}$是a*b的右逆元

又∵ $(b^{-1}*a^{-1})*(a*b)=b^{-1}*(a^{-1}*a)*b=e$

∴$b^{-1}*a^{-1}$是a*b的左逆元 ∴ $(a*b)^{-1}=b^{-1}*a^{-1}$。 #

5. 4 群与子群

群论是抽象代数发展充分的一个分支，广泛应用于计算,通讯，计算机科学，是本章的重点。

群（Group）

定义5-4.1：代数系统〈G，*〉，如果二元运算 *满足：

1) 封闭性，即∀a,b,∈G，a*b ∈G。
2) 结合律，即∀a,b,c∈G，a*（b*c）=（a*b）*c。
3) 存在幺元e，即∀a∈G，e*a=a*e=a。
4) G中每个元素存在逆元，∀a∈G，$\exists a^{-1}\in G$,使$a*a^{-1}=a^{-1}*a=e$。

则称〈G，*〉为群（Group）。

例： <R-{0}, x >是一个群。

群（Group）

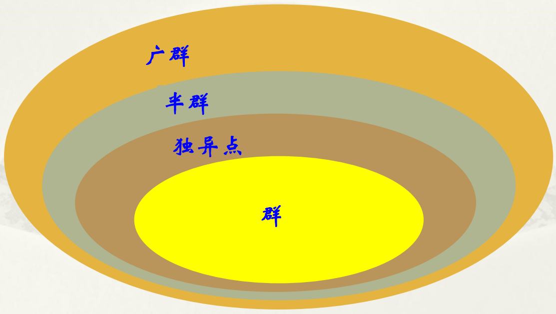
广群：　集合+运算+封闭性

半群：　集合+运算+封闭性+结合律

独异点：　集合+运算+封闭性+结合律+幺元

群：　集合+运算+封闭性+结合律+幺元+逆元

概念 汇总



阶数

定义5-4.2：设〈G，*〉为群，若G是有限集，称〈G，*〉为有限群，｜G｜称为群的阶数，若G是无限集，称〈G，*〉为无限群。

例：　<R-{0}, x >是一个无限群。

群的性质

有关代数系统，广群，半群和独异点的性质在群中全部成立，

例如，$(a*b)^{-1}=b^{-1}*a^{-1}$

例如，定理5-2.2: 设〈A，∗〉是一个代数系统，且集合A中元素的个数大于1。如果该代数系统中存在幺元e和零元θ，则θ ≠e。

定理5-4.1　群中不可能有零元。

证：当｜G｜=1，它的唯一元素视为幺元(而不视为零元)。

当|G|>1且〈G，*〉有零元θ，则∀x∈G，都有 x*θ=θ*x=θ≠e。

∴θ无逆元，这与G是群矛盾。　#

方程解唯一性

定理5-4.2：若〈G，*〉是一个群，则∀a，b∈G

a）存在唯一的x，使得a*x=b，

b）存在唯一的y，使得y*a=b。

证：

a）存在性：令$x=a^{-1}*b$，则$a*(a^{-1}*b)=a*a^{-1}*b=e*b=b$。

唯一性：若a*x’=b，则$\underbrace{a^{-1}*a}_{=e}*x' =a^{-1}*b$ ∴$x' =a^{-1}*b=x$。

b）略

消去律

定理5-4.3 若〈G，*〉是一个群，

则∀a，b，c∈G，有

(a) $a*b=a*c \Rightarrow b=c$

(b) $b*a=c*a \Rightarrow b=c$

（群上*满足消去律）

证：∵ $a*b=a*c$

$\Rightarrow a^{-1}*(a*b)=a^{-1}*(a*c)$

$\Rightarrow b=c$ #

置换

定义5-4.3：设S是一个非空集合，从集合S到S的一个双射，称为S的一个置换。

例如，S={a,b,c,d}，一个置换为

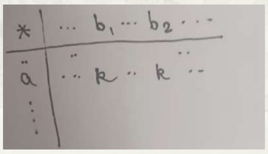
$$\begin{pmatrix} a & b & c & d \\ d & c & b & a \end{pmatrix}$$

置换

定理5-4.4：群〈G，*〉的运算表中的每一行或每一列是G中元素的一个置换。

证：① 先证运算表中每一行(列)中的元素不能出现二次(单射)。

∵若$a*b_1=a*b_2=k$，且$b_1\neq b_2$，与可约性(消去律)矛盾。



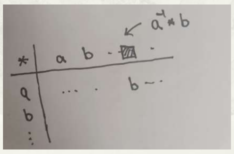
置换

定理5-4.4：群〈G，*〉的运算表中的每一行或每一列是G中元素的一个置换。

证：② 再证G中任一元素在任一行（列）中均出现（满射）。

∵考察对应于a的那一行，∀b∈G，则$b=a*(a^{-1}*b)$，

∴b出现在a那一行，由a，b任意性得证。

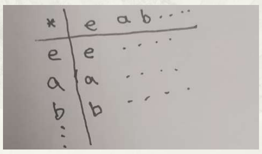


置换

定理5-4.4：群〈G，*〉的运算表中的每一行或每一列是G中元素的一个置换。且各个置换均不相同。

证：③因〈G，*〉中有幺元，

∴任二行（列）均不相同（即各个置换均不相同）。



例

① 一阶群仅有1个

*	e
e	e

② 二阶群仅有1个

*	e	a
e	e	a
a	a	e

③ 三阶群仅有1个

*	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

例

③ 三阶群仅有1个

表头

*	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

例

③ 三阶群仅有1个

e是幺元

*	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

zs1

例

③ 三阶群仅有1个

若a*b=b;
则a*b=e*b,
从而a = e, 矛盾
因此, a*b=e

*	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

zs2

例

③ 三阶群仅有1个

a*b=e
a, b 互逆

*	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

zs3

例

③ 三阶群仅有1个

*	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

④ 四阶群仅有2个

*	e	a	b	c
e	e	a	b	c
a	a	b	c	e
b	b	c	e	a
c	c	e	a	b

*	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

* ⑤ 五阶群仅有1个

*	e	a	b	c	d
e	e	a	b	c	d
a	a	b	c	d	e
b	b	c	d	e	a
c	c	d	e	a	b
d	d	e	a	b	c

* ⑥ 六阶群仅有2个

*	e	a	b	c	d	f
e	e	a	b	c	d	f
a	a	b	c	d	f	e
b	b	c	d	f	e	a
c	c	b	f	e	a	b
d	d	f	e	a	b	c
f	f	e	a	b	c	d

*	e	a	b	c	d	f
e	e	a	b	c	d	f
a	a	e	d	f	b	c
b	b	f	e	d	c	a
c	c	d	f	e	a	b
d	d	c	a	b	f	e
f	f	b	c	a	e	d

定理5-4.5：幺元是群中唯一的等幂元。

证：若x是等幂元素，即$x*x = x$，

则：$x = e*x = (x^{-1}*x)*x = x^{-1}*(x*x)$

$= x^{-1}*x = e$ #

回顾

* 定理5-4.1 群中不可能有零元。
* 方程解唯一性
* 消去律
* 置换
* 定理5-4.5：幺元是群中唯一的等幂元。

子群

定义5-4.5 设$<G,*>$为群，$S\subseteq G$，若$<S,*>$也构成群，则称$(S,*)$为$(G,*)$的子群(Subgroup)。

定义5-4.6 如果$S = \{e\}$或者$S = G$，则称$< S, * >$是$< G, * >$的平凡子群。

定理5－4.6 设$< G, * >$是一个群，$< S, * >$是$< G, * >$的一个子群，那么$< G, * >$的幺元e必定也是$< S, * >$的幺元.

证：设$< S, * >$的幺元为e'，则对于任意S中的元素x，都有

$e' * x = x = e * x$，

则$e' = e$。 #

子群的判定方法 1

定理 5－4.7： $<G,*>$是群，$H\subseteq G$且非空，如果H有限且*运算在H上封闭，那么$<H,*>$必定是$<G,*>$的子群。

(群：集合+运算+封闭性+结合律+幺元+逆元)

任取$a\in H$，若$a=e$，则$a^{-1}=e^{-1}=e\in H$。

若$a\neq e$,令 $S=\{a,a^2,\ldots\}$，因为运算*封闭，所以$S\subseteq H$。

由于H是有穷集，必有$a^i=a^j$ $(i<j)$，即$a^i=a^i*a^{j-i}$。

根据G中的消去律得：$a^{j-i}=e$ （H中存在幺元）

$j-i\geq 1$，

$j-i>1$时，由$a^{j-i-1}*a=e$ 和 $a*a^{j-i-1}=e$可知a^{j-i-1}为a的逆元；

$j-i=1$时，由$a^i=a^i*a^{j-i}$可知a即为幺元，幺元以自身为逆元；

从而证明了 $a^{-1}=a^{j-i-1}\in H$ （H中每个元素存在逆元） 。

61

子群的判定方法 2

定理5-4.8： $<G,*>$是群, $S\subseteq G$且非空,若$\forall a,b\in S$,有$a*b^{-1}\in S$，则$<S,*>$是$<G,*>$的子群。(S有限或无限)

证明： 首先证明G中的幺元也是S中的幺元

1） $\forall a\in S$，有$a*a^{-1}=e\in S$。

其次证明，S中的每一元素都有逆元

2） $\forall a\in S$，由于$e\in S$，则有$e*a^{-1}=a^{-1}\in S$。

最后证明封闭性

3） $\forall a,b\in S$，由2）可知$b^{-1}\in S$，

又因为$(b^{-1})^{-1}=b$，所以$a*(b^{-1})^{-1}=a*b\in S$。

故$<S,*>$是$<G,*>$的子群。 #

62

例2、若$<H,*>$，$<K,*>$是群$<G,*>$的子群，则$<H\cap K,*>$是$<G,*>$的子群。

证明：

设$\forall a,b\in H\cap K$，则$a,b\in H$、$a,b\in K$，

又因为$<H,*>$，$<K,*>$是群$<G,*>$的子群。

所以，$b^{-1}\in H$，$b^{-1}\in K$。

根据封闭性，$\therefore a*b^{-1}\in H$，$a*b^{-1}\in K$。即$a*b^{-1}\in H\cap K$。

由子群判别法2知：$<H\cap K,*>$是$<G,*>$的子群。

63

5.5 阿贝尔群与循环群

定义5-5.1： 设〈G，*〉为群，若*满足交换律，称〈G，*〉为阿贝尔群(或可交换群).

广群：集合+运算+封闭性

半群：集合+运算+封闭性+结合律

独异点：集合+运算+封闭性+结合律+幺元

群：集合+运算+封闭性+结合律+幺元+逆元

阿贝尔群：集合+运算+封闭性+结合律+幺元+逆元+交换律

64

例1、〈I，+〉是一个群，且为阿贝尔群，

证： ① 〈I，+〉运算封闭。

② 普通加法满足结合律。

③ 0为幺元。

④ $\forall a\in I$，$-a$是a的逆元。

⑤ 普通加法满足交换律。

例 2 〈Q_+，×〉是阿贝尔群

65

定理5-5.1 设〈G，×〉是一个群，则〈G，*〉是阿贝尔群的充要条件是：

$\forall a, b\in G$，有$(a*b)*(a*b) = (a*a)*(b*b)$

证： 充分性：若$\forall a, b\in G$,有$(a*b)*(a*b)=(a*a)*(b*b)$。

所以，$a^{-1}*(a*b)*(a*b)*b^{-1}=a^{-1}*(a*a)*(b*b)*b^{-1}$

$\therefore b*a=a*b$，∴〈G，*〉是阿贝尔群。

必要性：若〈G，*〉是阿贝尔群，则$\forall a, b\in G$，$a*b=b*a$。

$\therefore a*(a*b)*b=a*(b*a)*b$，

$\therefore (a*a)*(b*b) = (a*b)*(a*b)$。 #

66

循环群

定义5-5.2 设<G,*>是一个群,若在G中存在元素a，使得G中任意元素都由a的幂组成，则称<G,*>是一个**循环群**，元素a称为循环群<G,*>的**生成元**。

例，群{<0°,60°,120°,180°,240°,300°>，★}
其中，★是两个角度连续旋转，即“mod 360加”，
该群是一个循环群，其生成元是60°。

学生解题

定理5-5.2 任何循环群必定是阿贝尔群。

学生解题

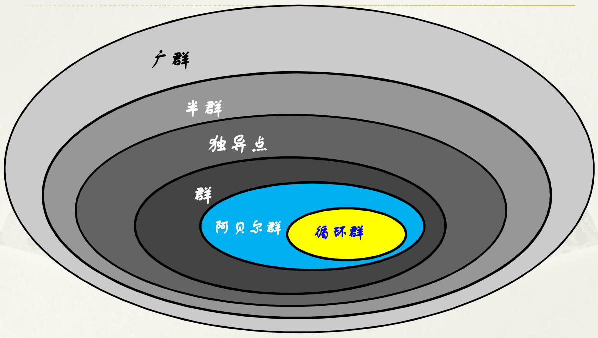
定理5-5.2 任何循环群必定是阿贝尔群。

证：设g是<G,*>的生成元,

则$\forall a,b\in G$, $a=g^r$, $b=g^s$ $(r,s\in I)$,

$a*b=g^r*g^s=g^{r+s}=g^{s+r}=g^s*g^r=b*a$。 #

概念 汇总



概念 汇总

广群: 集合+运算+封闭性

半群: 集合+运算+封闭性+结合律

独异点: 集合+运算+封闭性+结合律+幺元

群: 集合+运算+封闭性+结合律+幺元+逆元

阿贝尔群: 集合+运算+封闭性+结合律+幺元+逆元+交换律

循环群: 集合+运算+封闭性+结合律+幺元+逆元+交换律+生成元

元素的阶

定义： 设a是G中的一个元素，若∃正整数n，使得$a^n=e$，则**使得$a^n=e$的最小正整数n称为元素a的阶**(或称“a的周期”)，记为O(a)，并称a是有限阶的元素。

定理5-5.3：设$<G,*>$是由a生成的有限循环群，若G的阶为n，即$|G|=n$，则$G=\{a^1, a^2, \ldots, a^n=e\}$。其中$e$是幺元，$n$是$a^n=e$最小正整数(即$a$的阶)。

证：a) 证a的阶$\geqslant n$。先证：若$m<n$，则$a^m \neq e$。

（反证法） 若$m<n$，且$a^m=e$，$\forall a^k \in G$，$k=mq+r, 0 \leqslant r<m$，

$\therefore a^k=a^{mq+r}=a^{mq} \cdot a^r=(a^m)^q \cdot a^r=(e)^q \cdot a^r=a^r$，

$\therefore G$中最多有m个不同元素，这与$|G|=n$矛盾，所以a阶$\geqslant n$。

b)证G中的元素全不相同。

（反证法） 若$a^i=a^j (1 \leqslant i<j \leqslant n)$，　$a^{j-i}=e$。

$\because 0 \leqslant j-i<n$　$\therefore$这与a)矛盾。

c) $\because a^i \in G$且$|G|=n (1 \leqslant i \leqslant n)$，$\therefore G=\{a^1, \ldots, a^n\}$，

$\because$ 群G中必有幺元e $\therefore a$的阶$\leqslant n$　$\therefore a$的阶$=n$，即$a^n=e$

73

推论：$<G,*>$是群，对任何$a \in G$，有$(a^n)^{-1}=(a^{-1})^n$

规定1：$a^{-n}=(a^n)^{-1}=(a^{-1})^n$

规定2：$a^0=e$　$(e=a*a^{-1}=a^{1+(-1)}=a^0)$

回顾定义5-5.2　设$<G,*>$是一个群，若在G中存在元素a，使得G中任意元素都由a的幂（包含负幂次）组成，则称$<G,*>$是一个循环群，元素a称为循环群$<G,*>$的生成元。

74

例1. a) $<I,+>$是无限循环群，其中　是生成元。

（生成元不唯一）

b) $<\{5j \mid j \in I\},+>$是无限循环群，其中　是生成元。

75

例2.设$G=\{\alpha, \beta, \gamma, \delta\}$，G上二元运算*如下右表所示。证明$<G,*>$是循环群。

证：$\because \gamma^2=\beta, \gamma^3=\delta, \gamma^4=\alpha$ $\therefore$运算表可改写如下：

*	α	β	γ	δ
α	α	β	γ	δ
β	β	α	δ	γ
γ	γ	δ	β	α
δ	δ	γ	α	β

*	γ^4	γ^2	γ	γ^3
γ^4	γ^4	γ^2	γ	γ^3
γ^2	γ^2	γ^4	γ^3	γ
γ	γ	γ^3	γ^2	γ^4
γ^3	γ^3	γ	γ^4	γ^2

*	γ^4	γ	γ^2	γ^3
γ^4	γ^4	γ	γ^2	γ^3
γ	γ	γ^2	γ^3	γ^4
γ^2	γ^2	γ^3	γ^4	γ
γ^3	γ^3	γ^4	γ	γ^2

由上表看出$<G,*>$是一个循环群。

δ也是生成元，生成元不唯一

76

练习：

$<\{3n \mid n \in I\},+>$是$<I,+>$的子群，其中I为整数集。

(群：集合+运算+封闭性+结合律+幺元+逆元)

答案：p.194 例题3

77

5.7 陪集与拉格朗日定理

定义5-7.1 设$\langle G,*\rangle$是群，A和B是G的非空子集，则记$AB=\{a*b \mid a\in A, b\in B\}$为A和B的积；记$A^{-1}=\{a^{-1} \mid a\in A\}$为A的逆。

(群：集合+运算+封闭性+结合律+幺元+逆元)

例 设群$\langle I,+\rangle$，$A=\{1\}$，$B=\{0，2\}$，则$AB=\{1，3\}$，$A^{-1}=\{-1\}$。

陪集

定义5-7.2:设$\langle H,*\rangle$是群$\langle G,*\rangle$的子群，元素$a\in G$，则称$\{a\}H=\{a*h \mid h\in H\}$为元素a所确定的子群$\langle H,*\rangle$的左陪集，

$H\{a\}=\{h*a \mid h\in H\}$称为元素a所确定的子群$\langle H,*\rangle$的右陪集。

简记为aH或Ha，a称为代表元素。

(注：重点讨论左陪集，若*为加法，相当于对H进行一个平移的全局操作.)

例1.求出$\langle N_6,+_6\rangle$关于子群$\langle\{0,3\},+_6\rangle$的所有左陪集和右陪集，其中$N_6=\{0,1,2,3,4,5\}$。

$+_6$	[0]	[1]	[2]	[3]	[4]	[5]
[0]	[0]	[1]	[2]	[3]	[4]	[5]
[1]	[1]	[2]	[3]	[4]	[5]	[0]
[2]	[2]	[3]	[4]	[5]	[0]	[1]
[3]	[3]	[4]	[5]	[0]	[1]	[2]
[4]	[4]	[5]	[0]	[1]	[2]	[3]
[5]	[5]	[0]	[1]	[2]	[3]	[4]

例1.求出$\langle N_6,+_6\rangle$关于子群$\langle\{0,3\},+_6\rangle$的所有左陪集和右陪集，其中$N_6=\{0,1,2,3,4,5\}$。

解:令$H=\{0,3\}$,则

左陪集:

$0H=\{0,3\}=3H=\cdots$

$1H=\{1,4\}=4H=\cdots$

$2H=\{2,5\}=5H=\cdots$

右陪集:

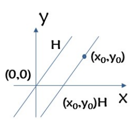
$H0=\{0,3\}=H3=\cdots$

$H1=\{1,4\}=H4=\cdots$

$H2=\{2,5\}=H5=\cdots$

从中可以看出：$\{0H,1H,2H\}$是G的一个划分。

例2



代数系统$\langle G,+\rangle$，其中$G=R\times R$，+定义为

$\langle x_1,y_1\rangle+\langle x_2,y_2\rangle=\langle x_1+x_2,y_1+y_2\rangle$，

显然$\langle G,+\rangle$是一个群。G的几何意义？二维平面

- $H=\{\langle x,y\rangle \mid y=2x\}$，容易验证$\langle H,+\rangle$是$\langle G,+\rangle$的一个子群。H的几何意义是？

  一条经过(0,0)的直线$y=2x$
- 对于$\langle x_0y_0\rangle\in G$，左陪集

  $\langle x_0,y_0\rangle H=\{\langle x+x_0,y+y_0\rangle \mid y=2x\}$的几何意义？

  一条经过（x_0,y_0）且平行于$y=2x$的直线

关于陪集

性质1: 设$\langle H,*\rangle$是$\langle G,*\rangle$的子群,$\forall a,b\in G$, 则

$$aH=bH \ \text{或}\ aH\cap bH=\Phi$$

证：设$aH\cap bH\neq\Phi$,即$\exists f\in aH\cap bH$。

$\therefore \exists h_1, h_2\in H$，使$f=a*h_1=b*h_2$，

$\therefore a=b*h_2*h_1^{-1}\in bH$。

$\forall x\in aH$，则$\exists h_3\in H, x=a*h_3=b*h_2*h_1^{-1}*h_3\in bH$

$\therefore aH\subseteq bH$，同理$bH\subseteq aH$。

$\therefore aH=bH$。 #

(注：所得结论对右陪集也平行成立；交空，呈现划分特征)

性质2：设<H,*>是<G,*>的子群，则子群<H,*>的任意左陪集的大小(即基数)相等。

证：$\forall a\in G$，$a*h_1, a*h_2\in aH$.

若$h_1\neq h_2$，则$a*h_1\neq a*h_2$.

$\therefore |aH|=|H|$。

∴H的任意陪集大小相同。

注：据性质1，可以证明：

1）设<H,*>是<G,*>的子群，$\forall a\in G$，则aH非空。(H有幺元)

2）设<H,*>是<G,*>的子群，$G=\cup_{a\in G}aH$. (aH包含a)

由左陪集性质可见：｛aH｝是G的一个划分。

拉格朗日定理

定理5-7.1　设<H,*>是群<G,*>的子群，那么$R=\{<a,b>|a\in G, b\in G, a^{-1}*b\in H\}$是一个等价关系，称为H的左陪集等价关系。($b\in aH$)

(a) 对于$a\in G$，若记$[a]_R=\{x|x\in G$, 且$<a,x>\in R\}$则$[a]_R=aH$。

(b)如果G是有限群，$|G|=n$, $|H|=m$,则 $m|n$

即：一个有限群<G, *>的子群<H, *>的阶|H| 只可能是G的阶|G|的因子。

等价关系：自反、对称且传递。

拉格朗日定理

- 定理5-7.1　设<H,*>是群<G,*>的子群,那么$R=\{<a,b>|a\in G, b\in G, a^{-1}*b\in H\}$是G上的一个等价关系，称为H的左陪集等价关系。

(1) $\forall a\in G$, $a^{-1}\in G$,有$a^{-1}*a=e\in H$，所以$<a,a>\in R$，因此R是自反的。

(2)若$<a,b>\in R$, 有$a^{-1}*b\in H$，$(a^{-1}*b)^{-1}=b^{-1}*a$, 因为H是G的子群，所以$(a^{-1}*b)^{-1}\in H$，即$b^{-1}*a\in R$, 所以$<b,a>\in R$,因此R是对称的。

(3)若$<a,b>, <b,c>\in R$, 则有$a^{-1}*b\in H$和$b^{-1}*c\in H$，所以$(a^{-1}*b)*(b^{-1}*c)\in H$，而$(a^{-1}*b)*(b^{-1}*c)=a^{-1}*c\in H$, 所以$<a,c>\in R$, 因此R是传递的.

综上，R是一个等价关系。

拉格朗日定理

- 定理5-7.1　设<H,*>是群<G,*>的子群,那么$R=\{<a,b>|a\in G, b\in G, a^{-1}*b\in H\}$是一个等价关系,称为H的左陪集等价关系。
- 对于$a\in G$，若记$[a]_R=\{x|x\in G$,且$<a,x>\in R\}$ 则$[a]_R=aH$.

$x\in [a]_R$

$\Leftrightarrow <a,x>\in R$

$\Leftrightarrow a^{-1}*x\in H$

$\Leftrightarrow x\in aH$。

拉格朗日定理

$|G|=n$, $|H|=m$, 则 $m|n$　(用到$[a]_R=aH$)

证明：由于R是G中的等价关系，可将G分成不同等价类(划分):

$$G=\bigcup_{i=1}^{k}[a_i]_R=\bigcup_{i=1}^{k}a_iH$$

- 由于这k个左陪集是两两不相交的基数相同的集合，所以有$|G|=|a_1H|+|a_2H|+\cdots+|a_kH|$　(1)
- 可知$|a_iH|=|H|$ $(i=1,2,\cdots,k)$，将这些代入式(1)得

$n=|G|=k|H|=km$

其中k为不同左(右)陪集的数目。定理得证。

拉格朗日定理

定理5-7.1：有限群<G,*>的任意子群<H,*>的阶数可以整除群G的阶数。

证：$\forall a\in G\Rightarrow a\in aH$,

$\therefore G=\cup_{a\in G}aH$。

由左陪集的性质知：H的左陪集集合是G的一个划分。

又$\forall a\in G$, $|aH|=|H|$。

∴|G|/|H|是G的划分的块数（即划分的秩）是个整数。

∴|H|可整除|G|。

推论

1. 质数阶的群没有非平凡子群($<\{e\},*>$,$<G,*>$ 称为 $<G,*>$ 的平凡子群)。

2. 有限群 $<G,*>$ 中的任何元素a的阶可整除|G|。

证:若 $a \in G$ 的阶是r(即 $a^r=e$),则 $\{e,a,a^2,a^3,\ldots,a^{r-1}\}$ 是G的子群。

3. 质数阶的群,一定是循环群。

证:设 $<G,*>$ 为质数阶群,则G的阶大于1(既不是质数也不是合数).

$\forall a \in G, a \neq e$,由推论2知:

a的阶数可整除|G|,但是|G|为质数,所以a的阶数等于群的阶数,

$\therefore \{a,a^2,\ldots,a^r\}=G$,(r为a的阶数)

$\therefore <G,*>$ 是循环群。

(有限群中的元素必有阶,且阶是有限的.)

例3.设K={e,a,b,c},在K上定义二元运算 * 如下表所示:证明〈K, *〉是一个群,但不是循环群。

*	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

证:由运算表可知,运算 * 是封闭的和可结合的。幺元是e,每个元素的逆是自身,所以〈K, *〉是群。又因为a,b,c都是二阶元素,故〈K, *〉不是循环群。

称〈K, *〉为Klein(克莱因)四元群。

例3.设K={e,a,b,c},在K上定义二元运算 * 如下表所示:证明〈K, *〉是一个群,但不是循环群。

*	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

证:由运算表可知,运算 * 是封闭的和可结合的。幺元是e,每个元素的逆是自身,所以〈K, *〉是群。又因为a,b,c都是二阶元素,故〈K, *〉不是循环群。(循环群有生成元,阶为4)

称〈K, *〉为Klein(克莱因)四元群。

例4.四阶群只有二个,一个是四阶循环群,另一个是Klein四元群。 ($|G|=n=4$, 元素的阶: 1, 2, 4)

证:1)设四阶群为<{e,a,b,c}, * >。其中e是幺元。当四阶群含有一个四阶元素时,这个群就是循环群。

2)当四阶群不含有四阶元素时,则由推论2可知,除幺元e外,a,b,c的阶数一定都是2。

假设a * b等于a,b或e,则b=e,a=e或a=b矛盾。所以a * b=c。

a*b=e=a*a, 则a=b

类似可证:b * a=c

a * c=c * a=b

b * c=c * b=a。

因此,这是一个Klein四元群。

*	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

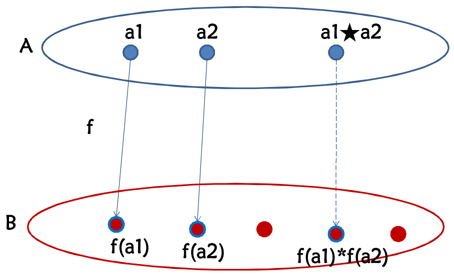
5.8 同态与同构

定义5-8.1 设 $<A,★>$ 和 $<B,*>$ 是两个代数系统,f是从A到B的映射,$\forall a,b \in A$,有 $f(a_1★a_2)=f(a_1)*f(a_2)$ 则称f是从 $<A,★>$ 到 $<B,*>$ 的一个同态映射,称 $<A,★>$ 同态于 $<B,*>$,记作 $<A,★> \sim <B,*>$。

把 $<f(A),*>$ 称为 $<A,★>$ 的一个同态象,其中 $f(A)=\{x \mid x=f(a), a \in A\}$(值域),包含于B(陪域)。

同态:乘积的象等于象的乘积,也就是f不仅将元素映射到元素,也将运算映射到运算.

示意图



例1 <I,×>是一个代数系统，

另一个代数系统<B, ⊙ >，其中B={正，负，零}，⊙运算表如下，

作映射f：I→B如下，

$$f(n)=\begin{cases}正 & n>0\\ 负 & n<0\\ 零 & n=0\end{cases}$$

⊙	正	负	零
正	正	负	零
负	负	正	零
零	零	零	零

显然，对于任意a，b属于I，有

f(a×b)=f(a)⊙f(b)，所以<I,×>同态于<B, ⊙ >

同态像的性质

广群：集合+运算+封闭性

半群：集合+运算+封闭性+结合律

独异点：集合+运算+封闭性+结合律+幺元

群：集合+运算+封闭性+结合律+幺元+逆元

阿贝尔群：集合+运算+封闭性+结合律+幺元+逆元+交换律

循环群：集合+运算+封闭性+结合律+幺元+逆元+交换律+生成元

同态像的性质

定理5-8.2 设f是代数系统<A, ★ >到代数系统<B, * >的同态,则

1)若<A, ★ >是半群,则<f(A), * >也是半群。

证:∀a,b,c∈f(A),∃x,y,z∈A,有a=f(x),b=f(y),c=f(z)，则

封闭性: a * b=f(x) * f(y)=f(x ★ y)∈f(A)

结合律: a * (b * c)=f(x) * (f(y) * f(z))

=f(x) * f(y ★ z)

=f(x ★(y ★ z))

=f((x ★ y) ★ z)=f(x ★ y) * f(z)

=(f(x) * f(y)) * f(z)=(a * b) * c

∴<f(A), * >是半群。

同态像的性质

2)若<A, ★ >是独异点,则<f(A), * >也是独异点.

证:∀a∈f(A), ∃x,有a=f(x). 则

a * f(e)=f(x) * f(e)=f(x★e)=f(x)=a，(右幺元)

f(e) * a=f(e) * f(x)=f(e ★ x)=f(x)=a。(左幺元)

∴f(e)是<f(A), * >的幺元

∴ <f(A), * >是独异点。

（幺元的象，就是象的幺元）

同态像的性质

3)若<A, ★ >是一个群,则<f(A), * >也是一个群.

证:∀f(x)∈f(A)，

f(x) * $f(x^{-1})$=$f(x★x^{-1})$=f(e)，(右逆元)

$f(x^{-1})$ * f(x)=$f(x^{-1}★ x)$=f(e)，(左逆元)

∴$f(x)^{-1}$=$f(x^{-1})$，即<f(A), * >也是一个群。

（逆元的象，就是象的逆元）

同态像的性质

4)若<A, ★>是阿贝尔群,则<f(A), * >也是阿贝尔群.

证：∀a,b∈f(A)

∃x,y∈A,使得：a=f(x),b=f(y)

由<A, ★ >是阿贝尔群可知：

x ★ y= y ★ x

故 a * b=f(x) * f(y)=f(x ★ y)

=f(y ★ x)=f(y) * f(x)=b * a （交换律）

即<f(A), * >也是阿贝尔群。

同态像的性质

总结：

1)同态像f（A）继承了原象代数系统A的所有性质。

2)若h是<A, ★ > → <B, * > 的同态映射，
$\langle B, * \rangle$不一定满足$\langle A, ★ \rangle$中的所有性质。
（陪域）

同构

定义5-8.2 设f是从代数系统$\langle A, ★ \rangle$到$\langle B, * \rangle$的同态，

如果f是满射，则称f为**满同态**；

如果f是入射，则称f为**单一同态**；

如果f是双射，则称f**同构映射**，此时代数系统A与B是**同构**的,记作$\langle A, ★ \rangle \cong \langle B, * \rangle$。

例1.a) $f: N \to N_k (k>0)$， $f(x)=x \bmod k$
是$\langle N,+\rangle$到$\langle N_k,+_k\rangle$的满同态.

证：设$x_1=lk+h_1, x_2=mk+h_2$ $(h_1,h_2<k)$，

则∵$f(x_1+x_2)=(x_1+x_2) \bmod k$

$=(h_1+h_2) \bmod k = h_1 +_k h_2 = f(x_1) +_k f(x_2)$。

∴$f(x_1+x_2)=f(x_1)+_k f(x_2)$。

又∵f是满射 ∴ f是$\langle N,+\rangle$到$\langle N_k,+_k\rangle$的满同态。

b）设f：$R \to R$定义为对任意$x \in R$，$f(x)=5^x$，那么f是从$\langle R,+\rangle$到$\langle R, \times \rangle$的单一同态。

c）设$H=\{7n，n \in I\}$，定义f：$I \to H$为对任意$n \in I$，有$f(n)=7n$，那么f是从$\langle I,+\rangle$到$\langle H,+\rangle$的一个同构。

例2.证$\langle R_+, \times \rangle$同构于$\langle R,+\rangle$。

证:i) 令 $h: R_+ \to R$, $h(x)=\lg x$

则因为对数函数单调增，∴h是单射。

$\forall y \in R, \exists x=10^y$，使$y=\lg 10^y=h(x)$，

∴h是满射。

∴h是从R_+到R的双射。

ii) $h(a \times b)=\lg(a \times b)=\lg a+\lg b=h(a)+h(b)$

∴$\langle R_+, \times \rangle$同构于$\langle R,+\rangle$。

定理5-8.1 代数系统之间的同构关系是等价关系。

证明：1）（自反性）设〈A, *〉为任一代数系统.

作恒等映射$f:A \to A$，则f是双射。并且$\forall a,b \in A$有：

$f(a * b)=a * b=f(a) * f(b)$。所以$\langle A, * \rangle \cong \langle A, * \rangle$。

2）（对称性）设$\langle A, * \rangle \cong \langle B, ☆ \rangle$。

则存在双射$f:A \to B$，并且$\forall a,b \in A$有： $f(a * b)=f(a) ☆ f(b)$。

所以$f^{-1}:B \to A$也是双射。$\forall y_1,y_2 \in B$，存在$x_1,x_2 \in A$，使得$f(x_1)=y_1, f(x_2)=y_2$。

故有：$f^{-1}(y_1 ☆ y_2)=f^{-1}(f(x_1) ☆ f(x_2))$

$=f^{-1}(f(x_1 * x_2))$

$=x_1 * x_2$

$=f^{-1}(y_1) * f^{-1}(y_2)$。

因此$\langle B, ☆ \rangle \cong \langle A, * \rangle$。

3）（传递性）设$\langle A, * \rangle \cong \langle B, ☆ \rangle$，$\langle B, ☆ \rangle \cong \langle C, \triangle \rangle$。

则存在双射$f:A \to B$和$g:B \to C$，故$g \circ f$也为双射。

$\forall a,b \in A$有： $g \circ f(a * b)=g(f(a) ☆ f(b))$

$=g(f(a)) \triangle g(f(b))$

$= g \circ f(a) \triangle g \circ f(b)$

所以，$\langle A, * \rangle \cong \langle C, \triangle \rangle$. #

同态核

定义5-8.3 设代数系统$\langle A, * \rangle$，如果f是$\langle A, * \rangle$到$\langle A, * \rangle$的同态，则称f**自同态**；

如果f是$\langle A, * \rangle$到$\langle A, * \rangle$的同构，则称f**自同构**.

定义5-8.4 设f是由群$\langle G, ★ \rangle$到群$\langle G', * \rangle$的同态，e'是G'的幺元，称$\ker(f)=\{x \mid x \in G \wedge f(x)=e'\}$为f的**同态核**。

> 把$\langle f(A), * \rangle$称为$\langle A, ★ \rangle$的一个同态象，其中$f(A)=\{x \mid x=f(a), a \in A\}$，包含于B。

例: $f:<I,+>\to<N_5,+_5>$, $\forall x\in N, f(x)=x \bmod 5$,
则f是同态吗?
$\forall x,y\in I$, $f(x+y)=(x+y) \bmod 5$
$=x \bmod 5+_5 y \bmod 5=f(x)+_5f(y)$,
$\therefore$ f是从$<I,+>$到$<N_5,+_5>$的同态。
f的**同态核**?
$ker(f)=\{x|x\in I\wedge f(x)=0\}=\{\ldots-10,-5,0,5,10,\ldots\}$。

定理5-8.3: f是群$<G,\star>$到$<G',*>$的同态,则
$<ker(f),\star>$必定是$<G,\star>$的子群;
若令K= ker(f),则a K=K a。
证: 1)**封闭性**: $\forall x,y\in ker(f)$,则$f(x)=e'$, $f(y)=e'$, (e'为G'的幺元)
$\therefore f(x\star y)=f(x)*f(y)=e'*e'=e'$,
$\therefore x\star y\in ker(f)$
幺元: $f(e)=e'$ (幺元的象,就是象的幺元),从而$e\in ker(f)$
逆元: $\forall x\in ker(f)$,则因$f(x^{-1})=f(x)^{-1}=(e')^{-1}=e'$
$\therefore x^{-1}\in ker(f)$ $\therefore$ $<ker(f),\star>$是群$<G,\star>$的子群。
2)令K=ker(f),$\forall a\in G$,设$f(a)=a'$, $\forall k_1\in K$
则$f(a\star k_1\star a^{-1})=f(a)*f(k_1)*f(a^{-1})=f(a)*f(a^{-1})=f(e)=e'$
即: $\exists k_2\in K$,有$a\star k_1\star a^{-1}=k_2$
$\therefore a\star k_1=k_2\star a$ $\therefore aK=Ka$ 即左陪集等于右陪集。

同余关系

定义5-8.5: $<A,\star>$是一个代数系统,R是A上的等价关系,若$\forall<a,b>,<c,d>\in R$都有
$<a\star c, b\star d>\in R$,
称R是A上关于★的**同余关系**,R将A划分的等价类称为**同余类**。

等价关系: 同色关系

同余关系: 涉及一种运算,即混色(50%+50%).
包含了这一运算的同色关系为同余.

同余关系

定义5-8.5: $<A,\star>$是一个代数系统,R是A上的等价关系,若$\forall<a,b>,<c,d>\in R$都有
$<a\star c, b\star d>\in R$,
称R是A上关于★的**同余关系**,R将A划分的等价类称为**同余类**。

等价关系: aRb当且仅当$a=b \pmod n$

同余关系: 若a_1Rb_1, a_2Rb_2, 则$(a_1+a_2)R(b_1+b_2)$. 因此R是一种同余

例1 代数系统$<A,\star>$,其中A={a, b, c, d},★运算表如下,定义在A上的等价关系
$R=\{<a,a>,<a,b>,<b,a>,<b,b>,<c,c>,<c,d>,<d,c>,<d,d>\}$
试验证R是A上的同余关系,并求R划分的同余类。
答: {a,b},{c,d}

★	a	b	c	d
a	a	a	d	c
b	b	a	c	d
c	c	d	a	b
d	d	d	b	a

例2: $<I,+>$,在I上定义R: $<x,y>\in R$当且仅当$|x|=|y|$,
问R是$<I,+>$的**等价关系**?是**同余关系**?
解:1)自反性: $\forall x\in I$, $|x|=|x|$ $\therefore <x,x>\in R$。
2)对称性: $\forall x,y\in I$, 若$<x,y>\in R$则$|x|=|y|$ $\therefore <y,x>\in R$。
3)传递性: $\forall x,y,z\in I$, 若
$<x,y>\in R$, $<y,z>\in R$ $\therefore |x|=|y|=|z|$ $\therefore <x,z>\in R$。
$\therefore$ R是一等价关系。
$\forall x_1,y_1,x_2,y_2\in I$, 若$<x_1,y_1>\in R$, $<x_2,y_2>\in R$,
$<x_1+x_2,y_1+y_2>\in R$ 不成立.
反例: 如$<1,-1>\in R$, $<2,2>\in R$但$<1+2,-1+2>\notin R$,
$\therefore$ R不是同余关系。
可见,等价关系未必都是同余关系。

定理5-8.4: 设<A,★>是一个代数系统，R是A上的一个同余关系，B={$A_1,A_2,\cdots,A_r$}是由R诱导的划分，则必存在运算*与同态映射f，使<B,*>是<A, ★>的同态象。

证:构造在B上运算*:

$\forall [a]_R,[b]_R \in B$， 有 $[a]_R * [b]_R = [a★b]_R$

构造映射

f: A→B，$\forall a \in A, f(a)=[a]_R$

再证f是一个同态映射:

$\forall x,y \in A, f(x★y)=[x★y]_R=[x]_R*[y]_R=f(x)*f(y)$，

∴f是从A→B的同态

又$\forall [a]_R \in B, \exists a \in A$有$f(a)=[a]_R$ ∴ f是满同态。证毕 。

集合上的同余关系可诱导一种划分，并进一步诱导一个从集合到划分的满同态映射。

定理5-8.5: 设f是代数系统<A, ★>到<B,*>的同态，定义A上的关系R:<a,b>∈R当且仅当f(a)=f(b)，那么，R是A上的一个同余关系。

证:1) 易证R是一个等价关系。

2) <a,b>∈R,<c,d>∈R,

∴f(a)=f(b),f(c)=f(d),

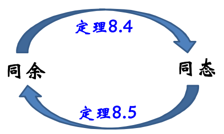
则f(a★c)=f(a)*f(c)=f(b)*f(d)=f(b★d),

∴<a★c, b★d>∈R。

∴R是A上的同余关系。

也即，任一同态映射可诱导一个同余关系

- 理解同态与同余之间的“诱导”



- 这是因为，其实 (教科书220页)
  - 同态象，可以看作是抽掉次要元素的情况下，对该系统的粗糙描述。
  - 同余类，也可以描述简要描述原系统的性态。

5.9 环与域

广群: 集合+运算+封闭性

半群: 集合+运算+封闭性+结合律

独异点: 集合+运算+封闭性+结合律+幺元

群: 集合+运算+封闭性+结合律+幺元+逆元

阿贝尔群: 集合+运算+封闭性+结合律+幺元+逆元+交换律

循环群: 集合+运算+封闭性+结合律+幺元+逆元+交换律+生成元

零元素暂无位置!(因为模型是乘法群而不是加法群)

5.9 环与域

同一个群<A,★>有两种模型解释:

将★当成乘法，记着 ·	将★当成加法，记着 +
幺元: e·a=a	零元: θ+a=a
逆元: $a \cdot a^{-1}=e$	负元: a+(-a)=θ
零元暂不强调	幺元不强调

5.9 环与域

定义5-9.1 代数系统<R,+,·>，若具有如下性质:

1) <R,+>是个阿贝尔群，(结合律, 幺元, 逆元, 交换律)
2) <R,·>是个半群， (结合律)
3) 乘法·对加法+可分配，即

$\forall a,b,c \in R$，$a\cdot(b+c)=a\cdot b+a\cdot c$，且$(b+c)\cdot a=b\cdot a+c\cdot a$，

称<R,+,·>是一个环。

约定: a的加法逆元记为-a，a+(-b)可简写为a-b。

重要约定（参考）

环内有两个运算，每个运算都可能有单位元、逆元等特殊元素。

为方便起见，做如下约定：

- 设$< A,+,\cdot >$是一个环，加群$< A,+ >$中的单位元通常记做0，称为零元（这个叫法是针对乘法的）。元素a在加群中的逆元记做$-a$，称为a的负元。如果乘法半群$< A,\cdot >$中有单位元，则称其为环A的单位元，记做1。如果乘法半群$< A,\cdot >$中某元素a有逆元，则称其为环A中元素a的逆元，记做a^{-1}。
- 可见，环中的单位元和逆元是针对乘法运算的，而加法运算中的单位元和逆元则称为零元和负元。
- 元素的倍数和幂定义为：$na = \underbrace{a+a+\cdots+a}_{n个a}$，$a^n = \underbrace{aa\ldots a}_{n个a}$

  且满足$(na)b = a(nb) = nab$，$a^n a^m = a^{n+m}$，$(a^n)^m = a^{nm}$

例1.

1) $<I,+,\times>$是个环。

2) $<N_k,+_k,\times_k>$是个环。

证： ①$<N_k,+_k>$是个阿贝尔群， 0是加法幺元，

②$<N_k,\times_k>$是个半群。

③$\forall a,b,c \in N_k$ $a\times_k(b+_k c)=a\times_k((b+c) \bmod k)$

$=(a\times(b+c)) \bmod k=(a\times b+a\times c) \bmod k$

$=(a\times b) \bmod k +_k (a\times c) \bmod k$ $=(a\times_k b)+_k(a\times_k c)$

关于环

定理5-9.1: 设$<A, +, \cdot>$是个环,$\forall a,b,c\in A$,

1) 环的加法幺元必为环的乘法零元，即 $\theta\cdot a=a\cdot\theta=\theta$。（完全扮演了零元角色）

证： $a\cdot\theta =a\cdot(\theta+\theta)=a\cdot\theta+a\cdot\theta$,由消去律可得： $a\cdot\theta=\theta$。

类似可证$\theta=\theta\cdot a$。

2) $(-a)\cdot b=a\cdot(-b)=-(a\cdot b)$

证:$(-a)\cdot b+a\cdot b=((-a)+a)\cdot b=\theta\cdot a=\theta$，

$\therefore (-a)\cdot b=-(a\cdot b)$。类似可证$a\cdot(-b)=-(a\cdot b)$。

3) $(-a)\cdot(-b)=a\cdot b$ (教科书 pp.224)

证:$(-a)\cdot(-b)=-a\cdot(-b)=a\cdot b$（利用2）的结果）

4) $a\cdot(b-c)=a\cdot b-a\cdot c$

证:$a\cdot(b-c)=a\cdot(b+(-c))=a\cdot b+a\cdot(-c)=a\cdot b+(-(a\cdot c))=a\cdot b-a\cdot c$

5) $(b-c)a=ba-ca$（类似4）的证明）

---

zs1 zs2

三种特殊的环

广群： 集合+运算+封闭性

半群： 集合+运算+封闭性+结合律

独异点： 集合+运算+封闭性+结合律+幺元

群： 集合+运算+封闭性+结合律+幺元+逆元

阿贝尔群：集合+运算+封闭性+结合律+幺元+逆元+交换律

定义5-9.2: 设$<R,+,\cdot>$是环，

若$<R,\cdot>$是可交换的，称$<R,+,\cdot>$为交换环。

若$<R,\cdot>$含幺元，称$<R,+,\cdot>$为含幺环。

若$\exists a,b\in A$，$a\neq\theta$，$b\neq\theta$，使$a\cdot b=\theta$，称$<A,+,\cdot>$是含零因子环，其中a,b称为零因子；否则称为无零因子环。

注：无零因子：$\forall a,b\in A$，$a\neq\theta, b\neq\theta$，则必有$a\cdot b\neq\theta$

例：$<I,+,\cdot>$是无零因子环；

$<N_4,+_4,\times_4>$是含零因子环：$2\times_4 2=2\times 2 \bmod 4 = 0$

无零因子环的判定

定理5-9.2 环$<A,+,\cdot>$是无零因子环当且仅当乘法消去律成立，也即对于$c\neq\theta$且$c\cdot a=c\cdot b$，必有$a=b$。

证明： 群的消去律是基于逆元存在性,而这里A是半群

1：若无零因子，设$c\neq\theta$且$c\cdot a=c\cdot b$，则

$c\cdot(a-b)=\theta$，则$a-b=\theta$，则$a=b$，即

消去律成立；

2：若消去律成立，即$c\neq\theta$且$c\cdot a=c\cdot b$，必有$a=b$，

即 $c\neq\theta$ 且$a\neq b$，必有$c\cdot a\neq c\cdot b$，（逆否命题）

即 $c\neq\theta$ 且$a\neq b$，必有$c\cdot(a-b)\neq\theta$，则无零因子

一个更特殊的环

定义5-9.3: 设$<A,+,\cdot>$是环，如果满足：

① $<A,+,\cdot>$既是交换环；

② $<A,+,\cdot>$还是含幺环；

③ $<A,+,\cdot>$且是无零因子环；

则称$<A,+,\cdot>$为整环。

例2. 1) $<I,+,\times>$是整环。

2) $<N_4,+_4,\times_4>$不是整环。

$<N_4,+_4,\times_4>$是含零因子环：$2\times_4 2=2\times 2 \bmod 4 = 0$

域

定义5-9.4：设代数系统$\langle A,+,\cdot\rangle$满足

1)$\langle A,+\rangle$是阿贝尔群；

2)$\langle A-\{\theta\},\cdot\rangle$是阿贝尔群；

3)运算·对+可分配，

则称$\langle A,+,\cdot\rangle$是域。

例

1) Q为有理数集合，$\langle Q,+,\times\rangle$是一个域。

R为实数集合，$\langle R,+,\times\rangle$是一个域。

C为复数集合，$\langle C,+,\times\rangle$是一个域。

2) I为整数集，$\langle I,+,\times\rangle$不是域。

(5，无乘法逆元)

例2. 1)$\langle I,+,\times\rangle$是整环。

---

zs3

关于域

定理5-9.3：域一定是整环。

$\langle A,+,\cdot\rangle$为域:

$\langle A,+\rangle$是阿贝尔群;

乘法·对加法+可分配;

$\langle A-\{\theta\},\cdot\rangle$是阿贝尔群--可交换，含幺，可逆$\Leftrightarrow$

$\langle A,\cdot\rangle$半群+可交换+含幺+除零，可逆

$\langle A,+,\cdot\rangle$为整环:

$\langle A,+\rangle$是阿贝尔群;

乘法·对加法+可分配;

$\langle A,\cdot\rangle$是半群+可交换+含幺+无零因子($\Leftrightarrow$除零，消去律)

关于域

定理5-9.3：域一定是整环。

证明：（除零，可逆$\Rightarrow$消去律）

设$\langle A,+,\cdot\rangle$是任一域。

对于$\forall a,b,c\in A$且$a\neq\theta$，

如果有$a\cdot b=a\cdot c$，则（1是乘法幺元）：

$b=1\cdot b=(a^{-1}\cdot a)\cdot b=a^{-1}\cdot(a\cdot b)=a^{-1}\cdot(a\cdot c)$

$=(a^{-1}\cdot a)\cdot c=1\cdot c=c$

因此，$\langle A,+,\cdot\rangle$是一个整环。

定理5-9.4 有限整环必是域。

证：（有限，除零，消去律$\Rightarrow$可逆）

设$\langle A,+,\cdot\rangle$是有限整环，$\forall a,b,c\in A$且$c\neq\theta$（证明c逆存在）.

若$a\neq b$，则由无零因子推出的消去律可知：$a\cdot c\neq b\cdot c$，

因为A为有限集，由运算封闭性

$\therefore$设$A-\{\theta\}=\{a_1,\ldots,a_n\}$，则$A-\{\theta\}=\{ca_1,\ldots,ca_n\}=c(A-\{\theta\})$。

$\therefore\forall c\in A,\exists d$有$c\cdot d=e$（整环含幺）$\therefore$ c逆元存在，即为d。

$\therefore\langle A-\{\theta\},\cdot\rangle$是阿贝尔群。

因为有限整环满足分配律，$\therefore\langle A,+,\cdot\rangle$是域。

- 无限整环未必是域。

例如，$\langle I,+,\times\rangle$是整环，却不是域！

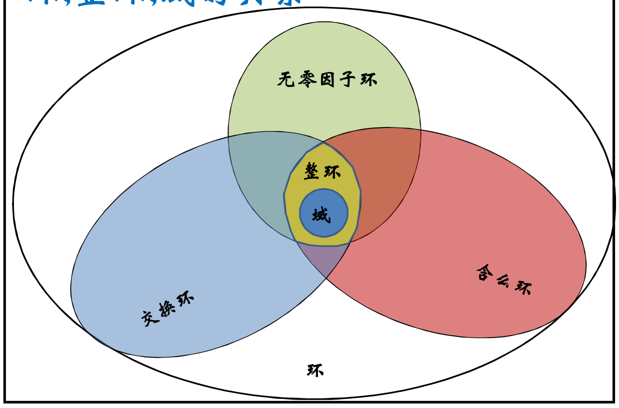
可见，域是一种特殊的整环。

2) I为整数集，$\langle I,+,\times\rangle$不是域。

(5，无乘法逆元)

例2. 1)$\langle I,+,\times\rangle$是整环。

环,整环,域的关系



环的同态

定义5-9.5: 设$<A,+,\cdot>$，$<B,\oplus,\odot>$是环， 若$\exists f: A\to B$，$\forall a,b\in A$ 有 $f(a+b)=f(a)\oplus f(b)$， $f(a\cdot b)=f(a)\odot f(b)$，称f是$<A,+,\cdot>$到$<B,\oplus,\odot>$的环同态。

定理5-9.5： 环的同态象必定是一个环。

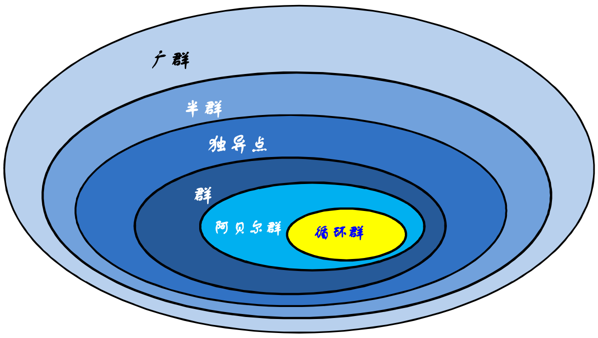
证:由群同态,半群同态知:是$<f(A),\oplus>$是阿贝尔群,$<f(A),\odot>$是半群，又因为 $f(a)\odot(f(b)\oplus f(c))$

$$=f(a)\odot(f(b+c)) =f(a(b+c))$$
$$=f(a\cdot b+a\cdot c) =f(a\cdot b)\oplus f(a\cdot c)$$
$$=f(a)\odot f(b)\oplus f(a)\odot f(c)$$ （分配律）

所以 $<f(A),\oplus,\odot>$是一个环。

对于域来说，该结论不成立。

本章总结



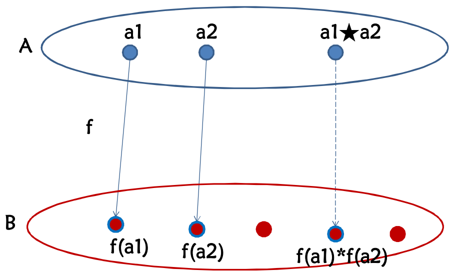
57

群的重要性质

拉格朗日定理

定理5-7.1: 有限群$<G,*>$的任意子群$<H,*>$的阶数可以整除群G的阶数。

同态与同构(关于运算的映射关系)



同余关系(关于运算的等价关系)

定义5-8.5: $<A,★>$是一个代数系统，R是A上的等价关系，若$\forall<a,b>,<c,d>\in R$都有

$<a★c, b★d>\in R$,

称R是A上关于★的同余关系，R将A划分的等价类称为同余类。

等价关系：同色关系

同余关系：涉及一种运算，即混色(50%+50%)，包含了这一运算的同色关系为同余。

5.9 环与域(关于两个运算的故事)

定义5-9.1 代数系统<R,+,·>，若具有如下性质:

1) <R,+>是个阿贝尔群，(结合律,幺元,逆元,交换律)

2) <R,·>是个半群，(结合律)

3) 乘法·对加法+可分配，即

$\forall a,b,c\in R$，$a\cdot(b+c)=a\cdot b+a\cdot c$，且$(b+c)\cdot a=b\cdot a+c\cdot a$，

称<R,+,·>是一个环。

约定：a的加法逆元记为-a，a+(-b)可简写为a-b。

环,整环,域的关系